Position #512318
IS Technical Services - Specialist
Application Security Analyst

POSITION SUMMARY

Under the general supervision of the Chief Information Security Officer (CISO), this position supports the Department of Employee Trust Funds (ETF) and its partners in information security matters related to application security to include those applications developed, purchased as a service, or used in the cloud by ETF.

The incumbent will utilize commercial-off-the-shelf and open-source application security tools such as, but not limited to, static code analyzers, dynamic code analyzers, or application traffic monitors to audit and report weaknesses and areas for improvement in current and future ETF applications. The incumbent will also make recommendations for security toolset improvements, recommend and work to implement security-related improvements to development processes, and provide production application security support. In addition, this position will assist in the development of custom tools and scripts to enhance security processes and systems for ETF.

The incumbent will combine extensive experience in applications development using programming languages, such as Java, with good secure coding practice. This position will also have knowledge of application server infrastructure, web server infrastructure, Linux/Unix environments, vulnerability scanners, penetration testing software, and other security-related tools.

This position requires a high level of responsiveness and customer service to be successful. This position is expected to create, promote, make full use of, and follow applicable ETF and state standards, policies, and best practices. This includes but is not limited to change management, issue tracking, business requirements elicitation, project management, security testing, etc. This position plays a key role in supporting ETF staff, third-party administrators, and employers.

This is a key position for recommending and establishing direction of information security policies and technical controls for IT systems and business applications.

GOALS and WORKER ACTIVITIES

40% GOAL A: Performance of responsibilities as ETF's application security specialist.

Worker Activity

- A1. Collaborate with application developers to select, develop, implement, maintain, and continuously improve ETF's application security-related information security controls.
- A2. Provide security-enhancing recommendations to development teams, project teams, and other stakeholders during all phases of application development or acquisition.
- A3. Provide security expertise at all phases of ETF's systems development life cycle (SDLC), which includes requirements gathering, design, development, testing, implementation, enhancements, and maintenance.

A4. Provide security-related expertise and advice to programmers in the remediation of application security issues which may compromise the confidentiality, integrity, or availability of ETF information systems and data assets.

A5. Work with developers to ensure ETF applications are developed to minimize the exposure of personal information to unauthorized parties.

A6. Collaborate with developers to ensure ETF applications are written and optimized to maximize the accuracy and consistency of data over its entire lifecycle.

A7. Support developers in ensuring ETF applications are built to be resilient so critical data and systems are readily available when needed.

A8. Using secure coding best-practices, including the use of code analyzer tools, collaborate with ETF application developers to help them build applications which are resistant and resilient to security breaches.

A9. Use standard business analysis techniques such as interviews, focus groups, or observation to identify and document security-related areas for improvement in existing application development processes or practices.

A10. Develop, implement, operate, and maintain tools and scripts to enhance and automate existing ETF security systems and processes.

30% GOAL B: Performance of information security governance, compliance, and audit activities with a focus on application security.

Worker Activity

B1. Verify, through various technical and process means, that ETF IT personnel and application development partners, vendors, and other stakeholders comply with industry-standard application security best-practices and ETF application security policy, standards, and procedures when building applications for ETF.

B2. Develop and coordinate security-related test plans that comply or align with industry-standard testing methodologies to ensure security-related application flaws are identified and documented.

B3. Develop, implement, and maintain procedures, guidelines, and related documentation regarding the implementation of application security policies and standards to ensure repeatable, standardized build processes.

B4. Support developers with documentation, mentoring, and training regarding ETF information security policies, procedures, and governance to ensure applications are built, configured, and operated securely.

B5. Use ETF and industry-standard change management processes to test releases of ETF's custom and vendor-delivered applications and review

them for compliance with ETF security policies and standards prior to being approved for production.

B6. Conduct continuous review of compliance requirements and security-related control objectives (such as those from the state Legislative Audit Bureau) and facilitate and document alignment of ETF's application development practices to those security-related control objectives.

20% GOAL C: Performance of application vulnerability and penetration assessments, identification of vulnerabilities, and recommendation and implementation of vulnerability remediation.

Worker Activity

C1. Perform manual and automated application security vulnerability and penetration assessments and properly document and communicate the vulnerabilities that are found through established service request processes.

C2. Facilitate vulnerability remediation solutions with developers that enhance security but also maintain business functionality.

C3. Conduct discovery to completion accountability for vulnerabilities by tracking, providing status for, verifying, and reporting completion of remediation service requests.

C4. Conduct validation of system vulnerability resolutions and work with BITS and DET personnel to ensure they are deployed to production in a timely manner.

C5. Provide expertise and advice for difficult remediation issues, to include helping affected business areas plan for downtime and other issues involved with closing vulnerabilities.

C6. Assist in the identification and documentation of application security vulnerabilities that cannot or should not be remediated, and the acknowledgement and acceptance of this risk through ETF's security governance process.

C7. Automate repeatable processes, such as vulnerability assessment and reporting, using batch programs and other scheduling technologies.

C8. Prepare status reports for management to highlight progress, identify obstacles, and recommend action in efforts to remediate identified vulnerabilities.

10% GOAL D. Participation in and leadership of security-related activities and projects. Performance of special assignments, consultation, training, and participation in employee development programs.

Worker Activity

D1. Support and otherwise carry out special assignments to respond to the needs of the Department.

D2. Coordinate and prepare special reports, reviews, and recommendations as requested.

D3. Assist other team members with other security activities, such as risk management, user awareness training, or security training.

D4. Represent ETF on task forces and committees to respond to state and agency needs.

D5. Orient new employees to information security standards, programming languages, utilities, procedures, standards, policies, practices and major application areas.

D6. Share knowledge with fellow BISM and BITS personnel and aid in areas of personal expertise.

D7. Promote the research, evaluation, and introduction of new technologies as appropriate to support agency business goals.

D8. Read books, periodicals, and internal documents to increase knowledge of information security for the organizational environment.

D9. Attend schools, training sessions, and workshops to improve data processing and management skills.

D10. Maintain knowledge of state-of-the-art software and information security technology through independent study and reading, classes, and hands-on training.

D11. Research and evaluate new tools and technologies and make recommendations on potential benefits of such tools and technologies for ETF staff.

D12. Additional duties as assigned.

(Rev. 05/2018)

Knowledge, Skills, and Abilities

1. Extensive knowledge and expert skills with major programming and scripting languages.
2. Extensive knowledge of application security best practices.
3. Experience with SDLC methodologies such as Agile and Waterfall and application development best practices.
4. Experience utilizing OWASP Top 10 and similar guidance to provide better security for business systems.
5. Knowledge and experience with vulnerability scanners and penetration testing software.
6. Ability to develop secure workflow and test procedures.
7. Knowledge of tools such as Web Scarab, Burp, Tamper Data, Wireshark, etc.
8. Knowledge of good security practices for all phases of application development.
9. Knowledge of the common vulnerabilities such as cross site scripting, SQL injection, insufficient transport layer protection, cross-site request forgery, HTTP response splitting, and fingerprinting.
10. Excellent written and oral communication skills.
11. Skills for effective use of MS-Office products (Word, Excel, PowerPoint).
12. Excellent ability to effectively collaborate and work with other technicians, project managers and business staff.
13. Demonstrated ability to work effectively with business partners and customers to solve business challenges while balancing the need for confidentiality, integrity, and availability of ETF's data and business systems.
14. Skilled in all levels of software testing for security and able to apply information security principles and concerns to those tests.
15. Full-spectrum understanding of information security processes, controls, technologies, and strategies.
16. Demonstrated commitment to fostering a diverse working environment.
17. Solid understanding of common and emerging information security attack vectors, penetration methods and countermeasures.
18. Demonstrated ability to work independently and as part of a team of peers and to support and contribute to a multidiscipline team environment.
19. Knowledge of conflict resolution and incident escalation.
20. Demonstrated ability to solve complex problems, convey both oral and written instruction, and handle multiple task interruptions while providing services in a professional and courteous manner.
21. Proven ability to work with diverse audiences and translate technical jargon into non-technical information.
22. Ability to resolve issues in a variety of complex situations which require complex judgments and solutions based on sophisticated analytical thought.
23. Understanding of technical concepts and technologies such as application security, secure coding concepts, endpoint security, edge technologies, enterprise management platforms and malware defenses.
24. Knowledge of project management principles, methods, and practices.

25. Experience and knowledge of techniques to effectively communicate and influence technical staff, functional users, and various levels of management.
26. Understanding of threat, vulnerability and risk management methodologies and tools.